Assurance report

Lessor Group

ISAE 3402 type 2 assurance report on IT general controls for the period 1 April 2023 to 31 March 2024 related to Lessor Group's provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management

July 2024

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of contents

Section 1: Lessor Group's statement

The purpose of this description is to provide information for Lessor Group's entities (Lessor A/S, Danske Lønsystemer A/S and Emply International ApS) customers and their stakeholders. Throughout this document, the term Lessor Group refers to these companies.

The description has been prepared for customers who have used Lessor Group's provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management, and their auditors who have a sufficient understanding to consider the description along with other information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

Lessor Group is using subservice organisations Netic A/S, NetNordic Denmark A/S, PostNord Strålfors A/S, Post Danmark A/S, Contractbook ApS, Bogholdergruppen.DK ApS, Compaya A/S, Trifork Security A/S and Interlogic Danmark ApS. This assurance report is prepared in accordance with the carve-out method and Lessor Group's description does not include control objectives and controls within Netic A/S, NetNordic Denmark A/S, PostNord Strålfors A/S, Post Danmark A/S, Contractbook ApS, Bogholdergruppen.DK ApS, Compaya A/S, Trifork Security A/S and Interlogic Danmark ApS. Certain control objectives in the description can only be achieved, if the subservice organisations' controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by subservice organisations.

Some of the control areas, stated in Lessor Group's description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers are suitably designed and operationally effective with Lessor Group's controls. This assurance report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

Lessor Group confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to Lessor Group's provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management processing of customer transactions throughout the period 1 April 2023 to 31 March 2024. The criteria used in making this statement were that the accompanying description:

(i) Presents how the system was designed and implemented, including:
- The type of services provided
- The procedures within both information technology and manual systems, used to manage IT general controls
- Relevant control objectives and controls designed to achieve these objectives
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary, to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by us alone
- Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to IT general controls

(ii) Contains relevant information about changes in the IT general controls, performed throughout the period 1 April 2023 to 31 March 2024

(iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and functioning throughout the period 1 April 2023 to 31 March 2024 if relevant controls with the subservice organisation were operationally effective and the customers have performed the complementary user entity controls, assumed in the design of Lessor Group's controls throughout the period from 1 April 2023 to 31 March 2024. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved

(iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 April 2023 to 31 March 2024

Allerød, 3 July 2024
Lessor Group ApS
on behalf of Lessor A/S, Danske Lønsystemer A/S and Emply International ApS

Henrik Møller
Chief Executive Officer

Section 2: Independent service auditor's assurance report on the description of controls, their design and operating effectiveness

To: Lessor Group (Emply International ApS, Danske Lønsystemer A/S and Lessor A/S) their customers and their auditors.

Scope

We have been engaged to report on a) Lessor Group's description in Section 3 of its system for delivery of Lessor Group's provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management throughout the period 1 April 2023 to 31 March 2024 and about (b+c)) the design and operational effectiveness of controls related to the control objectives stated in the description. Lessor Group is using the subservice organisations Netic A/S, NetNordic Denmark A/S, PostNord Strålfors A/S, Post Danmark A/S, Contractbook ApS, Bogholdergruppen.DK ApS, Compaya A/S, Trifork Security A/S and Interlogic Danmark ApS. This assurance report is prepared in accordance with the carve-out method and Lessor Group's description does not include control objectives and controls within Netic A/S, NetNordic Denmark A/S, PostNord Strålfors A/S, Post Danmark A/S, Contractbook ApS, Bogholdergruppen.DK ApS, Compaya A/S, Trifork Security A/S and Interlogic Danmark ApS. Certain control objectives in the description can only be achieved if the subservice organisations' controls, assumed in the design of our controls, are appropriately designed and operationally effective. The description does not include control activities performed by subservice organisations.

Some of the control objectives stated in Lessor Group's description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers have been appropriately designed and works effectively with the controls with Lessor Group. The report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

Lessor Group's responsibility

Lessor Group is responsible for preparing the description (Section 3) and accompanying statement (Section 1) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, Lessor Group is responsible for providing the services covered by the description; stating the control objectives; and for the design, implementation, and effectiveness of operating controls for achieving the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark. Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibility

Our responsibility is to express an opinion on Lessor Group's description (Section 3) as well as on the design and operation of the controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by International Auditing and Assurance Standards Board.

This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation in Section 3. We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a service organisation

Lessor Group's description in Section 3, is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the systems that each individual customer may consider important in their own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Furthermore, the projection of any functionality assessment to future periods is subject to the risk that controls with service provider can be inadequate or fail.

Opinion

Our opinion has been formed based on the matters outlined in this report. The criteria we used in forming our opinion were those described in Lessor Group's statement in Section 1 and based on this, it is our opinion that:

(a) The description of the IT general controls, as they were designed and implemented throughout the period 1 April 2023 to 31 March 2024, is fair in all material respects.
(b) The controls related to the control objectives stated in the description were suitably designed throughout the period 1 April 2023 to 31 March 2024 in all material respects, if controls with subservice organisations were operationally effective and if the customers have designed and implemented the complementary user entity controls assumed in the design of Lessor Group's controls during the period 1 April 2023 to 31 March 2024
(c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, have operated effectively throughout the period 1 April 2023 to 31 March 2024.

Description of tests of controls

The specific controls tested, and the nature, timing and results of these tests are listed in the subsequent main Section 4 including control objectives, test, and test results.

Intended users and purpose

This assurance report is intended only for customers who have used Lessor Group and the auditors of these customers, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves. This information serves to obtain an understanding of the customers' information systems, which are relevant for the financial reporting.

Copenhagen, 3 July 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

Section 3: Description of Lessor Group's services in connection with provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management and related IT general controls

Introduction

The purpose of this description is to provide information for Lessor Group's entities' (Lessor A/S, Danske Lønsystemer A/S and Emply International ApS) customers and their stakeholders. Throughout this document, the term Lessor Group refers to these companies.

The object of this description is to provide information to Lessor Group's customers and their auditors concerning the requirements laid down in the international auditing standard for assurance reports on the controls at a service organisation (ISAE 3402).

The infrastructure in scope of the description is Lessor Group's datacentre with Linux-servers.

Lessor Group and our services

Lessor Group offers a wide range of solutions within payroll and HR administration, shop floor management, time recording and workforce management.

Lessor Group's organisation and responsibility

Lessor Group has a clear and transparent corporate structure and employs over 350 employees.

The organisational structure of the Lessor Group includes the departments Administration, Finance, Development, Support, IT-security and IT Operations as well as various product departments.

The employees of the Lessor Group are thus responsible for the support of our own products as well as the hosting infrastructure. The support teams handle all incoming questions. They either solve the problems or pass on the task to the Operations Department for further processing.

Thus, the Operations Department acts as second line support and monitors existing operating solutions and other tasks associated with the day-to-day management of our hosting environment.

Risk assessment

IT risk analysis: Lessor Group's produced a risk analysis. On an annual basis or in case of significant changes, the group carries out a risk assessment of the assets of the Lessor Group. Both internal and external factors are taken into consideration.

The risk analysis provides an assessment of all risks identified. The risk analysis is updated on a yearly basis or in case of significant changes to ensure that the risks associated with the services provided are minimised to an acceptable level.

The responsibility for IT risk assessments lies with the CIO of the company who also approves the risk analysis.

Handling of security risks

Risk management procedure: We have implemented a scoring system for risks associated with the delivery of our services.

We assess the risks which we believe we are facing point by point. We make use of a simple calculation method for this purpose: "probability %" * "impact %".

The acceptable level goes to 20 %. We continuously assess if we can reduce the risks and take initiatives to address these risks.

Security policy

IT security policy

IT security policy document: We have defined our quality standards system based on the general objective of providing our customers with a stable and secure service. To comply with the objectives, we have implemented policies and procedures which ensure that our supplies are uniform and transparent. Our IT security policy is produced in accordance with ISO 27002:2013 and applies to all employees and all deliveries.

Our methodology for the implementation of controls is defined with reference to ISO 27002:2013 (guidelines for information security management) and is thus divided into the following control areas:

- Information security policies
- Organisation of information security
- Employee safety
- Asset management
- Conditional access
- Cryptography
- Physical security and environmental safeguards
- Operational safety
- Communication security
- Purchase, development, and maintenance of systems
- Supplier relationships
- Information security breach management
- Information security aspects related to emergency and restoration management
- Compliance

We continue to improve both policies, procedures, and operations.

Evaluation of the IT security policy: We update the IT security policy regularly and at least once a year. The IT security policy is approved by the CEO.

Organisation of information security

Internal organisation

Delegation of responsibility for information security: Our organisation is divided into different areas of responsibility. We have prepared a number of detailed responsibility and role descriptions for employees on all levels. Confidentiality has been established for all parties involved in our business. The confidentiality is ensured via employment contracts.

Separation of functions: Through on-going documentation and processes, we try to eliminate or minimise the dependence on key management personnel. Tasks are assigned and defined via procedures for managing the operational services.

Contact with special interest groups: The operating staff subscribes to newsletters from e.g., DK-CERT and other sources to keep informed about the emerging security threat landscape.

Mobile equipment and teleworking

Mobile equipment and communication: We have made it possible for our employees to work from home via a VPN connection with two factor authentication. Portable units are protected by HDD passwords, log-in information, and HDD encryption. Mobile devices (smart phones, tablets etc.) can be used for the synchronisation of emails and the calendar.

Remote access: Only authorised persons are granted access to our network, systems and data. Access to corporate resources is protected with two factor authentication.

Human resource security

Prior to employment

Screening: We have implemented procedures for the recruitment of staff and thoroughly examine the curriculum vitae of the applicant to ensure that we employ the right candidate regarding background and skills. Furthermore, we ensure that employees have clean criminal records.

Conditions of employment: The general terms of employment, e.g., confidentiality related to the customers and personal circumstances, are specified in the employment contracts/job descriptions of all employees in which, among other things, the termination of employment and sanctions following security breaches are also described.

During employment

Management's responsibility: All new employees sign a contract prior to commencement of their employment. The contract provides that the employee must comply with the policies and procedures existing at any time. The contract/job description clearly defines the responsibility and role of the employee.

Awareness of and training activities related to information security: Our assets are first of all our employees. We encourage our operating staff to maintain their qualifications, educations, and certifications through training courses, lectures, and other relevant activities to ensure that the employees concerned can be kept up to date with security and be aware of new threats.

Sanctions: The general terms of employment, e.g., confidentiality related to the customers' and personal circumstances, are specified in the employment contracts of all employees in which, among other things, the termination of employment and sanctions following security breaches are also described.

Responsibility related to the termination of employment: When an employee terminates, a procedure will be initiated to ensure that the employee returns all relevant assets, e.g., portable devices etc. and that the access to buildings, systems and data are withdrawn. The overall responsibility to ensure all control procedures upon termination of employment lies with the CEO of the company. The documentation related to the termination of employment is available in electronic form in the human resources department.

Asset management

Responsibility for assets

List of assets: Servers and network equipment including configuration are registered to be used for documentation purposes and to gain an overview of equipment etc. To secure against unauthorised access and to ensure the transparency of the structure, we have prepared some documents describing the internal network including units, naming of units, logical division of the network etc. The documentation for equipment is updated on a regular basis and reviewed at least once a year by our operating staff.

Ownership of assets: Central network units, servers, peripheral units & systems are owned by operating staff members of Lessor Group.

Acceptable use of assets: This subject is described in the employee handbook.

Return of assets: When an employee terminates, a procedure will be initiated to ensure that the employee returns all relevant assets and that the access to buildings, systems and data is being withdrawn. The overall responsibility to ensure all control procedures upon termination of employment lies with the CEO of the company. The documentation related to the termination of employment is available in electronic form in the human resources department.

Classification of information

We ensure appropriate protection of information of importance to the organisation and our customers. We make sure that all data are labelled and classified and is only processed based on documented processes.

Access control

Access control requirements

Conditional access policies: The way the granting of access is handled is described in a policy document. The policy is part of our IT security policy.

User access administration

Procedures for creation and deletion of user profiles: The user profiles of our customers are created solely due to the wishes of our customers. In some of the systems, the end customer himself creates his user profile without interference Lessor Group's employees. Our own users are created as super users to ensure that our support teams can provide professional service. All user profiles must be personally identifiable. The access to passwords for accounts which only are used by systems (service users) are limited to few authorised persons.

Grant of Rights: The granting of privileges is controlled in accordance with the regular user administration process. Privileges are only granted on a need-to-basis.

Handling of confidential login information: Personal login information is known only by the employee and subject to a password policy to ensure the complexity.

Evaluation of user access rights: Periodically, i.e., once a year, we review the internal systems of the company including user profiles and access levels to ensure that the procedure related to the termination of employment is followed and that the customers' data cannot be accessed by former employees of Lessor Group.

User responsibility

Use of confidential password: The IT security policy provides that all employee passwords must be personal and that only the user knows the password. Passwords for service accounts etc. which cannot be used for logging in, and which are not changed for systemic reasons are stored in a separate system. Only a limited number of employees can access this system.

Control of access to systems and data

Limited access to data: The access for our employees is differentiated. Only systems, servers and data which are relevant to the area of work of each single employee are accessible.

System for the administration of passwords: All employees are subject to restrictions as regards the passwords to customer systems as well as the customers' own systems. All users have passwords which are subject to restrictions related to the creation of the passwords. Some of our systems require that the password is complex and changed regularly. In other systems, the customer himself determines the change frequency and complexity of the password.

Physical security

Secure areas: All customer facing services are hosted at a datacentre provider who has processes to ensure only accredited personnel has access.

Cryptography

We ensure the proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. We have policies on how we manage encryption keys and encryption techniques.

Operational safety

Change management

Change management: All changes follow an implemented change management process and are documented in Jira.

Capacity management: We have established a monitoring system for monitoring capacity constraints. All incidents follow an implemented incident management process.

Protection against malware

Measures against malware: We use a number of sophisticated security tools and have a SOC/SIEM implemented.

Backup

Backup of data: We ensure that we will be able to recreate systems and data in an appropriate and correct manner in accordance with the agreements concluded with our customers. We have, for that purpose, developed a test to re-establish systems and data.

Backups of our customers' data take place with us. Backup copies are saved in electronic form on a physical location other than the data centre.

Logging and monitoring

Incident logging: Network traffic and server logs are monitored and logged. Security logs are forwarded to our SIEM solution.

Administrator and operator logs: The administrator logging process is performed simultaneously with the ordinary logging process.

Time synchronisation: We make use of Internet NTP servers for synchronisation of all servers.

Managing software in operating systems: Via our patch process we ensure that only approved and tested updates are being installed. All patching follows a patch management procedure.

Managing technical vulnerabilities: Safety warnings from DK-CERT, version 2 (or others) are monitored and analysed. If relevant, they are installed on our internal systems within one month from the date of issue. Our internal solutions are subject to ongoing risk assessments.

Communication security

Network measures: All traffic, incoming as well as outgoing, is filtered by the firewall rules and advanced IPS tools.

Ensuring network services: The customers access our systems via https. Data transferred from our systems to external partners are IP whitelisted and, if this is possible, sent via encrypted data protocols.

Network division: Our network is divided into service segments to ensure independence between the offered services. Furthermore, test and production environments are divided into two segments.

Incident management

We ensure a consistent and effective approach to information security breach management, including communication of security incidents and vulnerabilities. We have policies in place to ensure that employees know how security breaches are defined, managed, and reported. This policy also instructs that employees are required to report information security weaknesses.

Business continuity management

Emergency planning: Lessor Group has prepared an emergency plan for the handling of an emergency. The emergency plan is anchored in the IT risk analysis and maintained at least once a year following the performance of the analysis.

The plan and the procedures are anchored in our operating documentation and procedures.

Testing, maintenance and re-evaluation of emergency plans: The plan is tested once a year as a part of our emergency preparedness procedure to ensure that the customers, at the lowest possible level, will be affected by an emergency situation.

Redundancy: We seek to ensure that all services are redundant to make sure that we, in the shortest possible time, will be able to re-establish the production environment in a new environment in case of non-repairable errors in the production environment. We continue to focus on this area.

Compliance

Review of information security

Independent evaluation of information security: An evaluation will be carried out by an external IT auditor when preparing the annual ISAE 3402 report.

Compliance with security policies and standards: We carry out internal audits once a year in order to test if our internal policies and procedures are followed. The audits include all services and the infrastructure as well as other areas, if necessary.

Changes implemented during the period

No significant changes have been implemented during the period.

Complementary user entity controls

Lessor Group's customers are, unless otherwise agreed, responsible for establishing connection to Lessor Group's servers.

Furthermore, the customers of the Lessor Group are, unless otherwise agreed, responsible for:

- administration of their own user profiles
- their own Internet connection
- own data

Section 4: Control objectives, controls, and service auditor testing

Purpose and scope

A description and the results of our tests based on the tested controls appear from the tables on the following pages. To the extent that we have identified significant weaknesses in the control environment or deviations therefrom, we have specified this.

This statement is issued according to the carve-out method and therefore does not include controls of Lessor Group's subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by Lessor Group's customers, are not included in this report.

Tests performed

We performed our test of controls at Lessor Group, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Lessor Group regarding controls. Inquiries have included questions on how controls are being performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls during the audit period, is assessed by sample testing.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

Test results

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general controls with Lessor Group.

A.5 Information security policies

A.5.1 Management direction for information security
Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations

No.	*Lessor Group's control*	*Grant Thornton's test*	*Test results*
5.1.1	*Policies for information security* A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties.	We have inspected that the information security policy has been approved by management, published, and communicated to employees and relevant stakeholders. We have inspected that the information security policy has been reviewed and approved by management.	No deviations noted.
5.1.2	*Review of policies for information security* The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.	We have inquired into the procedure for regular review of the information security policy. We have inspected that the information security policy is reviewed, based on updated risk assessments to ensure that it still is suitable, adequate, and efficient.	No deviations noted.

A.6 Organisation of information security

A.6.1 Internal organisation
Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation

No.	*Lessor Group's control*	*Grant Thornton's test*	*Test results*
6.1.1	*Information security roles and responsibilities* All information security responsibilities are defined and allocated.	We have inspected an organisation chart showing the information security organisation. We have inspected the description of roles and responsibilities within the information security organisation.	No deviations noted.
6.1.2	*Segregation of duties* Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisations' assets.	We have inspected documentation for segregation of duties. We have inspected general organisation chart for the organisation.	No deviations noted.
6.1.4	*Contact with special interest groups* Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.	We have inspected documentation that appropriate contact with special interest groups has been maintained.	No deviations noted.

A.7 Human ressource security

A.7.1 Prior to employment
Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered

No.	*Lessor Group's control*	*Grant Thornton's test*	*Test results*
7.1.1	*Screening* Background verification checks on all candidates for employment is being carried out in accordance with relevant laws regulations and ethics and are proportional to the business requirements the classification of the information to be accessed and the perceived risks.	We have inspected the procedure for screening of new employees. We have, by sample test, inspected documentation that screening documentation is being obtained on new employees during the audit period.	No deviations noted.
7.1.2	*Terms and conditions of employment* The contractual agreements with employees and contractors are stating their and the organisation's responsibilities in information security.	We have inspected the procedure for onboarding new employees. We have, by sample test, inspected documentation that new employees have been informed about their roles and responsibilities in information security.	No deviations noted.

A.7.3 Termination and change of employment Control objective: To protect the organisation's interests as part of the process of changing or terminating employment			
No.	***Lessor Group's control***	***Grant Thornton's test***	***Test results***
7.3.1	*Termination or change of employment responsibility* Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor, and enforced.	We have inspected the procedure for offboarding. We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment or contract. We have inspected documentation that information security responsibilities and duties that remain valid after termination or change of employment have been defined and communicated. We have, by sample test, inspected that employment contracts with employees include confidentiality agreement and that it is still valid after termination of contract.	No deviations noted.

A.8 Asset management

A.8.1 Responsibility for assets Control objective: To identify organisational assets and define appropriate protection responsibilities			
No.	***Lessor Group's control***	***Grant Thornton's test***	***Test results***
8.1.1	*Inventory of assets* Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained.	We have inspected asset listings.	No deviations noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	We have inspected list of asset ownership.	No deviations noted.

No.	Lessor Group's control	Grant Thornton's test	Test results
8.1.3	*Acceptable use of assets* Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented, and implemented.	We have inspected the rules for acceptable use of assets.	No deviations noted.
8.1.4	*Return of assets* All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement.	We have inspected the procedure ensuring return of assets. We have, by sample test, inspected that assets are being returned from terminated employees.	No deviations noted.

A.8.2 Classification of information Control objective: To ensure an appropriate protection of information considering the value of the information to the organisation.			
No.	**Lessor Group's control**	**Grant Thornton's test**	**Test results**
8.2.1	*Classification* Information is classified in terms of legal requirements value criticality and sensitivity to unauthorised disclosure or modification.	We have inspected guidelines for classification of information. We have inspected that assets are classified, and that risks have been assessed.	No deviations noted.

A.9 Access control

A.9.1 Business requirements of access control
Control objective: To limit access to information and information processing facilities

No.	Lessor Group's control	Grant Thornton's test	Test results
9.1.1	*Access control policy* An access control policy has been established, documented, and reviewed based on business and information security requirements.	We have inspected the access control policy. We have inspected that the policy has been reviewed and approved by management.	No deviations noted.
9.1.2	*Access to network and network services* Users are only being provided with access to the network and network services that they have been specifically authorised to use.	We have inspected that a procedure for granting access to network and network services has been established. We have inspected list of users with access to network and network services. We have inquired into whether access is based on the employees' work-related needs.	No deviations noted.

A.9.2 User access management
Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

No.	Lessor Group's control	Grant Thornton's test	Test results
9.2.1	*User Registration and de-registration* A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inspected that formalised procedures for user registration and de-registration have been established. We have, by sample test, inspected that the users' access rights have been approved. We have, by sample test, inspected that resigned users' access rights have been revoked.	No deviations noted.

No.	Lessor Group's control	Grant Thornton's test	Test results
9.2.2	*User access provisioning* A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services.	We have inspected, that a procedure for user administration has been established. We have, by sample test, inspected that user accesses have been assigned according to the access management and control procedure. We have inquired into whether any users have changed roles or jobs during the period.	No deviations noted.
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have inspected the procedures for allocation, use and restrictions of privileged access rights. We have inspected a list of privileged users and we have inquired into whether access rights have been allocated based on a work-related need. We have inspected that privileged user accesses are personally identifiable. We have inspected that periodical review of privileged access rights is being performed.	No deviations noted.
9.2.5	*Review of user access rights.* Asset owners are reviewing user's access rights at regular intervals.	We have inspected the procedure for regular review and assessment of access rights. We have inspected, that review and assessment of access rights is being performed on a yearly basis.	No deviations noted.
9.2.6	*Removal or adjustment of access rights* Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inquired into procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected that resigned employees have had their access rights cancelled.	No deviations noted.

A.9.3 User responsibilities Control objective: To make users accountable for safeguarding their authentication information			
No.	***Lessor Group's control***	***Grant Thornton's test***	***Test results***
9.3.1	*Use of secret authentication information.* Users are required to follow the organisations' s practices in the use of secret authentication information.	We have inspected guidelines for the use of secret passwords. We have inspected, that the implemented password policy is according to established guidelines.	No deviations noted.

A.9.4 System and application access control Control objective: To prevent unauthorised access to systems and applications			
No.	***Lessor Group's control***	***Grant Thornton's test***	***Test results***
9.4.1	*Information access restriction* Access to information and application system functions has been restricted in accordance with the access control policy.	We have inspected guidelines and procedures for securing access restriction to application system functions. We have inspected list of users with access to information and operation of application systems, and we have inquired into whether the users have a work-related need.	No deviations noted.
9.4.2	*Secure logon procedures* Access to systems and applications is controlled by procedure for secure logon.	We have inspected the procedure for secure logon. We have inspected, that MFA has been established in connection with logon.	No deviations noted.
9.4.3	*Password management system* Password management systems are interactive and have ensured quality passwords.	We have inquired into whether policies and procedures require quality passwords. We have inquired into whether systems for administration of access codes are configured in accordance with the requirements.	No deviations noted.

A.10 Cryptography

A.10.1 Cryptographic controls
Control objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information

No.	Lessor Group's control	Grant Thornton's test	Test results
10.1.1	*Policy on the use of cryptographic controls* A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have inspected the policy for the use of encryption. We have inspected list of updates and review of policies, and procedures where the policy for cryptography is included.	No deviations noted.
10.1.2	*Key management* A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.	We have inquired into the policies for administering cryptographic keys, that supports the company's use of cryptographic techniques. We have inspected that cryptographic keys are active, and that their renewal is being followed up on.	No deviations noted.

A.11 Physical and environmental security

A.11.1 Secure areas
Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities

No.	Lessor Group's control	Grant Thornton's test	Test results
11.1.1	*Physical security perimeter* Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.	We have inspected the procedure for physical protection of facilities and security perimeters. We have inspected relevant locations and their security perimeters to establish whether security measures have been implemented to prevent unauthorised access.	No deviations noted.

No.	Lessor Group's control	Grant Thornton's test	Test results
11.1.2	*Physical entry control* Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	We have inspected access points to establish, whether personal access cards are used to gain access to the office. We have inspected lists of employees with physical access to servers. We have inspected that yearly review of employees with physical access to the servers are conducted.	No deviations noted.

A.12 Operations security

A.12.1 Operational procedures and responsibilities
Control objective: To ensure correct and secure operation of information processing facilities

No.	Lessor Group's control	Grant Thornton's test	Test results
12.1.1	*Documented operating procedures.* Operating procedures have been documented and made available to all users.	We have inspected that requirements for documentation and maintenance of operating procedures have been established. We have inspected that documentation for operating procedures is updated and accessible to relevant employees.	No deviations noted.
12.1.2	*Change management* Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled.	We have inspected the procedure for changes in information processing facilities and systems. We have, by sample test, inspected documentation that change requests are being managed according to the established procedure.	No deviations noted.
12.1.3	*Capacity management* The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.	We have inspected the procedure for monitoring use of resources and adjustments of capacity, to ensure future capacity requirements We have inspected that relevant platforms are included in the capacity requirement procedure.	No deviations noted.

No.	Lessor Group's control	Grant Thornton's test	Test results
12.1.4	*Separation of development-, test- and operations facilities.* Development testing and operational environments are separated to reduce the risks of unauthorised access or changes to the operational environment.	We have inspected network chart, where separation of development-, test- and operations is described. We have inspected technical documentation that used system environments have been separated.	No deviations noted.

A 12.2 Protection from malware Control objective: To ensure that information and information processing facilities are protected against malware			
No.	**Lessor Group's control**	**Grant Thornton's test**	**Test results**
12.2.1	*Control against malware* Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.	We have inspected guidelines for controls against malware. We have inspected that controls against malware have been implemented.	No deviations noted.

A.12.3 Backup Control objective: To protect against loss of data			
No.	**Lessor Group's control**	**Grant Thornton's test**	**Test results**
12.3.1	*Information backup* Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy.	We have inspected that the backup procedure has been reviewed and updated during the period. We have inspected the backup configuration. We have, by sample test, inspected that backups are taken in accordance with the procedure. We have inspected documentation that a restore test has been carried out.	No deviations noted.

A.12.4 Logging and monitoring Control objective: To record events and generate evidence			
No.	***Lessor Group's control***	***Grant Thornton's test***	***Test results***
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	We have inspected the procedure for logging. We have inspected the log of manually registered incidents. We have inspected the user access log.	No deviations noted.
12.4.2	*Protection of log information* Logging facilities and log information are being protected against tampering and unauthorised access.	We have inspected the procedure for logging. We have inspected that logs are protected against tampering and unauthorised access. We have inspected the log of manually registered incidents. We have inspected the user activity log.	No deviations noted.
12.4.3	*Administrator and operator logs* System administrator and system operator activities have been logged and the logs are protected and regularly reviewed.	We have inspected procedures concerning logging of activities performed by system administrators and system operators. We have inspected that system administrators' and system operators' actions are being logged on servers and database systems.	No deviations noted.
12.4.4	*Clock synchronisation* The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source.	We have inquired into procedures for synchronisation against a reassuring time server. We have inspected, that synchronisation against a reassuring time server, has been implemented.	No deviations noted.

A.12.5 Control of operational software Control objective: To ensure the integrity of operational systems			
No.	***Lessor Group's control***	***Grant Thornton's test***	***Test results***
12.5.1	*Installation of software on operational systems* Procedures are implemented to control the installation of software on operational systems.	We have inspected the procedure for patching and upgrade on systems, and that is has been reviewed and updated during the period. We have inspected documentation that relevant systems are updated and patched according to specific requirements in the procedure.	No deviations noted.

A.12.6 Technical vulnerability management Control objective: To prevent exploitation of technical vulnerabilities			
No.	***Lessor Group's control***	***Grant Thornton's test***	***Test results***
12.6.1	*Management of technical vulnerabilities* Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	We have inspected the procedure regarding gathering and evaluation of technical vulnerabilities. We have inspected documentation for the setup of vulnerability scans.	No deviations noted.

A.13 Communications security

A.13.1 Network security management
Control objective: To ensure the protection of information in networks and its supporting information processing facilities

No.	Lessor Group's control	Grant Thornton's test	Test results
13.1.1	*Network controls* Networks are managed and controlled to protect information in systems and applications.	We have inspected that requirements for operating and control of network, including requirements and regulations about encryption, segmentation, firewalls, intrusion detection and other relevant security measures have been defined. We have inspected documentation for network design.	No deviations noted.
13.1.2	*Security of network services* Security mechanisms service levels and management requirements of all network services are identified and included in network services agreements whether these services are provided in-house or outsourced.	We have inspected documentation that security measures have been implemented for remote access to the network.	No deviations noted.
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inspected network charts, showing segregation of development-, test, and operations environments. We have inspected technical documentation that system environments are being segregated.	No deviations noted.

A.15 Supplier relationships

15.2 Supplier service delivery management
Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements

No.	Lessor Group's control	Grant Thornton's test	Test results
15.2.1	*Monitoring and review of third-party services* Organisations are regularly monitoring review and audit supplier service delivery.	We have inspected, that review and assessment of relevant audit reports on significant subservice organisations have been performed.	No deviations noted.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements
Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses

No.	*Lessor Group's control*	*Grant Thornton's test*	*Test results*
16.1.1	*Responsibilities and procedures* Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	We have inspected the procedure for manging security incidents. We have inspected that the procedure has been reviewed and updated during the period.	No deviations noted.
16.1.2	*Reporting information security events* Information security events are being reported through appropriate management channels as quickly as possible.	We have inspected guidelines for reporting of information security incidents. We have, by sample test, inspected that information security incidents are being reported through appropriate management channels.	No deviations noted.
16.1.3	*Reporting security weaknesses* Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	We have inspected guidelines for reporting of information security weaknesses. We have, by sample test, inspected that employees have reported weaknesses or suspected weaknesses in information systems and services.	No deviations noted.
16.1.4	*Assessment of and decision on information security events* Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have inspected procedure for assessment of information security incidents. We have, by sample test, inspected that information security incidents have been managed according to the procedure.	No deviations noted.
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have inspected the procedure for managing information security incidents. We have, by sample test, inspected that information security incidents have been handle in accordance with the procedure.	No deviations noted.

No.	Lessor Group's control	Grant Thornton's test	Test results
16.1.6	*Learning from information security incidents* Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have inquired about problem management function which analyses information security incidents in order to reduce probability of recurrence. We have, by sample test, inspected that knowledge is gathered from information security incidents and are used in the mitigation of similar incidents.	No deviations noted.

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity
Control objective: Information security continuity should be embedded in the organisation's business continuity management systems

No.	Lessor Group's control	Grant Thornton's test	Test results
17.1.1	*Planning information security continuity* Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been decided upon.	We have inspected that the contingency plan has been approved by management.	No deviations noted.
17.1.2	*Implementing information security continuity* Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained.	We have inspected that the contingency plan is maintained and updated as needed. We have inspected documentation that the contingency plan is accessible to relevant employees.	No deviations noted.
17.1.3	*Verify review and evaluate information security continuity* The established and implemented information security continuity controls are verified on a regular basis to ensure that they are valid and effective during adverse situations.	We have inspected documentation that risk areas in the contingency plan have been tested during the period.	No deviations noted.

A.18 Compliance

A.18.2 Information security reviews
Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures

No.	*Lessor Group's control*	*Grant Thornton's test*	*Test results*
18.2.1	*Independent review of information security* Processes and procedures for information security) (control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.	We have inspected documentation that independent review of the information security has been performed.	No deviations noted.
18.2.2	*Compliance with security policies and standards* Managers are regularly reviewing the compliance of information processing and procedures within their area of responsibility with the appropriate security policies standards and any other security requirements.	We have inspected the list of internal controls regarding compliance with policies and standards. We have, by sample test, inspected documentation that the internal controls concerning compliance with policies and procedures, have been performed.	No deviations noted.
18.2.3	*Technical compliance review* Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards.	We have, by sample test, inspected documentation that review has been performed for technical compliance with policies and standards. We have inspected that penetration test have been conducted and that a follow up on the findings have been made.	No deviations noted.